Τ. 1 (2021)
E-ISSN: 2732-6004
Available online at: http://ejournals.lib.auth.gr/infolawj/

# ΕΠΙΚΑΙΡΟΤΗΤΑ

## Α. ΕΠΙΘΕΣΗ RANSOMWARE COLONIAL PIPELINE: ΟΙ ΔΙΩΚΤΙΚΕΣ ΑΡΧΕΣ ΣΤΙΣ ΗΠΑ ΑΝΕΚΤΗΣΑΝ ΤΜΗΜΑ ΑΠΟ ΤΑ ΚΑΤΑΒΛΗΘΕΝΤΑ ΛΥΤΡΑ

Την 07.05.2021 η εταιρία Colonial Pipeline που εδρεύει στο Τέξας και μεταφορά υγρά καύσιμα μέσω αγωγού στις Νοτιοανατολικές πολιτείες των ΗΠΑ δέχθηκε κυβερνοεπίθεση με ιό τύπου ransomware που είχε ως στόχο τον εξοπλισμό που διαχειρίζονται τον αγωγό, με αποτέλεσμα να διακοπεί η λειτουργία του. Οι δράστες ζήτησαν λύτρα για να αποκαταστήσουν τη βλάβη στο ποσό των 4,4 εκ. δολαρίων που καταβλήθηκε στο ψηφιακό νόμισμα Bitcoin. Η ομοσπονδιακή αστυνομία στις ΗΠΑ ανακοίνωσε ότι την επίθεση έκανε η εγκληματική ομάδα DarkSide που έχει την έδρα της στη Ρωσία και η οποία είχε υποκλέψει δεδομένα από την ως άνω δεδομένα 100 GB, μια ημέρα πριν από την κυβερνοεπίθεση.

Ωστόσο, στις 07.06.2021, το Υπουργείο Δικαιοσύνης των ΗΠΑ κατέσχεσε τμήμα των λύτρων, ήτοι 2,3 εκ. δολάρια, ανακτώντας τον κωδικό για το ξεκλείδωμα του ηλεκτρονικού πορτοφολιού των κρυπτονομισμάτων, μετά από διάταξη που εξέδωσε Δικαστήριο στο Σαν Φρανσίσκο για την απόκτηση πρόσβασης σε έναν μισθωμένο διακομιστή, στον οποίο φιλοξενούνταν το ψηφιακό πορτοφόλι του δράστη/δραστών.

Πληροφορίες: capital.gr, 8-6-2021, Wikipedia, λήμμα: Colonial Pipeline cyber attack.

## Β. ΠΑΡΟΥΣΙΑΣΗ ΣΥΜΠΕΡΑΣΜΑΤΩΝ ΤΗΣ ΕΡΕΥΝΑΣ ΤΗΣ ΕΕ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΚΑΤΑΣΤΑΣΗ ΤΟΥ ΕΛΕΥΘΕΡΟΥ ΑΝΤΑΓΩΝΙΣΜΟΥ ΣΤΟΝ ΤΟΜΕΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (IOT)

### 01. Εισαγωγή

Η Ευρωπαϊκή Επιτροπή ενίοτε διεξάγει έρευνες σε τομείς οικονομικής δραστηριότητας, όταν προκύπτουν ενδείξεις παραβίασης του ελεύθερου

Τ. 1 (2021)
E-ISSN: 2732-6004
Available online at: http://ejournals.lib.auth.gr/infolawj/

ανταγωνισμού. [1] Τα πορίσματα χρησιμεύουν στη βαθύτερη κατανόηση των χαρακτηριστικών και των ζητημάτων του πεδίου της υπό έρευνας δραστηριότητος και στη χάραξη της κατάλληλης ρυθμιστικής πολιτικής.

Ο σκοπός της έρευνας δεν είναι η στόχευση μεμονωμένων εταιρειών, αλλά η εις βάθος κατανόηση του διαδικτυακού οικοσυστήματος του διαδικτύου των πραγμάτων (Internet of Things, IoT) υπό τη σκοπιά του καταναλωτή τέτοιου είδους προϊόντων και υπηρεσιών.[2]

02. Η σημερινή κατάσταση της αγοράς IoT

Τα προκαταρκτικά στοιχεία του τομέα IoT υποδεικνύουν μια τάση εμφάνισης όλο και περισσότερων «έξυπνων» συσκευών, με αποτέλεσμα οι καταναλωτές να διαθέτουν μια ευρεία γκάμα επιλογής και χρήσης τέτοιου είδους συσκευών εντός και εκτός της οικίας τους. Ωστόσο η χρήση τους εξαρτάται κατά μεγάλο βαθμό από την προσφερόμενη διεπαφή χρήστη (User Interface) και ειδικότερα από τους φωνητικούς βοηθούς (Voice Assistants). [3] Επί του παρόντος υπάρχουν ελάχιστοι φωνητικοί βοηθοί, οι κυριότεροι των οποίων είναι μόνο τρεις, ήτοι Alexa, Google Assistant και Siri.

Η κυριότερη διεπαφή χρήστη εντοπίζεται στο χώρο των φορητών εφαρμογών, υποδεικνύοντας την τάση των καταναλωτών, να χρησιμοποιούν τις φορητές τους συσκευές για πρόσβαση σε υπηρεσίες IoT. Όμως και στο χώρο των λειτουργικών συστημάτων φορητών συσκευών εντοπίζεται μεγάλη συγκέντρωση, με την προσφορά να περιορίζεται, κυρίως, στα συστήματα Android και iOS.

03. Ο ρόλος των φωνητικών βοηθών

Οι υπηρεσίες φωνητικών βοηθών εντοπίζονται σε όλη σχεδόν τη γκάμα των προσφερόμενων προϊόντων και υπηρεσιών και οι μεγαλύτεροι σε μέγεθος συμμετέχοντες στην αγορά έχουν παρουσία σε αυτόν τον τομέα. Εντοπίζεται, επομένως, μια αυξανόμενη τάση προς τη δημιουργία ολοκληρωμένων λύσεων IoT προς τους καταναλωτές. [4] Οι περισσότεροι συμμετέχοντες στην έρευνα δήλωσαν αδυναμία σχεδιασμού νέων ανταγωνιστικών προϊόντων και υπηρεσιών λόγω του

[1] Άρ. 17 του Κανονισμού 01/2003.
[2] Η έρευνα «Internet of Things Preliminary report» διαθέσιμη εδώ.
[3] Βλ. Internet of Things Preliminary report, 2.2.2 “User Interaction”
[4] Ibid 3.7 “Key Findings”

Τ. 1 (2021)
E-ISSN: 2732-6004
Available online at: http://ejournals.lib.auth.gr/infolawj/

απαγορευτικού κόστους σχεδιασμού νέων φωνητικών βοηθών και λόγω της καθετοποιημένης δομής των μεγαλύτερων ανταγωνιστών τους. Οι τελευταίοι διαθέτουν ένα τεράστιο οικοσύστημα προϊόντων, π.χ. κινητών τηλεφώνων, λειτουργικών συστημάτων και φωνητικών βοηθών, το οποίο λειτουργεί συνδυαστικά και ενίοτε αποκλειστικά με τις δικές τους συσκευές IoT, περιορίζοντας τις επιλογές των καταναλωτών. [5]

04. Η διαδραστικότητα

Η χρησιμότητα του οικοσυστήματος των IoT εξαρτάται σε μεγάλο βαθμό από τη διαδραστικότητα μεταξύ διαφορετικών κατασκευαστών προϊόντων και υπηρεσιών σύννεφου (cloud providers). Ωστόσο η επίτευξη της απαιτούμενης διαδραστικότητας απαιτεί πέρα από σημαντικές επενδύσεις και την πρόσβαση στα υπάρχοντα λειτουργικά συστήματα κινητών συσκευών. [6] Η πρόσβαση παρέχεται μέσω μιας εφαρμογής προγραμματισμού (Application Programming Interface, API), η οποία, ωστόσο σχεδιάζεται από τους ίδιους τους κατασκευαστές των λειτουργικών συστημάτων με τέτοιο τρόπο, ώστε η πρόσβαση τρίτων σε αυτά να είναι ασύμφορη ή εξαιρετικά δύσκολη, π.χ. με όρους μη διαπραγματεύσιμους.[7]

05. Η πρόσβαση στην αγορά IoT

Η πολυδιάστατη παρουσία των μεγαλύτερων συμμετεχόντων τόσο στο software όσο και στο hardware καθιστά εξαιρετικά αμφίβολη τη βιωσιμότητα μικρών και ανεξάρτητων παικτών λόγω της de facto περιορισμένης πρόσβασής τους στην αγορά. Η τελευταία οφείλεται, κυρίως, στο γεγονός ότι η χρησιμότητα του οικοσυστήματος IoT εξαρτάται σε μεγάλο βαθμό από τη διαδραστικότητα περισσοτέρων προϊόντων και υπηρεσιών, η οποία επιτυγχάνεται μέσω της συνεργασίας διαφορετικών τεχνολογιών.[8]

Συνεπώς μια ανεξάρτητη και απομονωμένη τεχνολογία έχει λιγότερες πιθανότητες χρήσης της από τον καταναλωτή σε σύγκριση με μια καθιερωμένη - προεγκατεστημένη τεχνολογία σε ένα ευρύ οικοσύστημα IoT. Για παράδειγμα ο χρήστης μια συσκευής iOS δεν πρόκειται να εγκαταλείψει το λειτουργικό του

[5] Ibid 4.3 Barriers to entry and expansion, Figure 14: Barriers to entry or expansion, όπου αναλύονται σε γράφημα τα εμπόδια στην πρόσβαση τρίτων.
[6] Ibid 5.2 “Key role of consumer IoT technology platforms”
[7] Ibid 5.3 “Overview of technical interoperability in the consumer IoT sector”
[8] Ibid 6.4 “The role of standards and protocols vs proprietary technologies in consumer IoT”

Τ. 1 (2021)
E-ISSN: 2732-6004
Available online at: http://ejournals.lib.auth.gr/infolawj/

σύστημα, προκειμένου να αγοράσει ένα προϊόν μη συμβατό με το τελευταίο. Αντιθέτως θα προτιμήσει προϊόντα ή υπηρεσίες που είναι συμβατά με αυτό.[9]

06. Δεδομένα χρηστών IoT

Η διαδραστικότητα στο χώρο του IoT επιτυγχάνεται με την ανταλλαγή δεδομένων μεταξύ των διαφόρων συσκευών και υπηρεσιών. Οι ροές αυτών των δεδομένων ενίοτε είναι μεγάλες, καθώς περιλαμβάνουν πέρα από τα καθαρά τεχνολογικά και τα προσωπικά δεδομένα των χρηστών και απευθύνονται σε πολλούς τρίτους αποδέκτες. Η έρευνα κατέδειξε ότι η πρόσβαση τρίτων στα δεδομένα IoT ενδεχομένως να περιορίζεται ή να υπαγορεύεται από τους παρόχους φωνητικών βοηθών και λειτουργικών συστημάτων, ακόμη και αν οι τελευταίοι δεν είναι οι κατασκευαστές των προϊόντων, εκμεταλλευόμενοι την αναγκαιότητα των υπηρεσιών τους για την ορθή λειτουργία του IoT.

Τα είδη των δεδομένων που υφίστανται επεξεργασία, αφορούν τα αναγκαία για την ομαλή λειτουργία, δεδομένα τεχνικών λαθών ή λειτουργικής απόδοσης, δεδομένα εξατομίκευσης της εμπειρίας του χρήστη κλπ. Παρά ταύτα οι συμμετέχοντες ανέφεραν ότι η δημιουργία προφίλ με τις συνήθειες και τις προτιμήσεις των χρηστών για σκοπούς εμπορικής προώθησης ή διαφήμισης αποτελεί δυνητικά μια σημαντική πηγή εκμετάλλευσης και προσπορισμού κερδών.[10] Η Επιτροπή σημειώνει ότι οι συσκευές και υπηρεσίες IoT χαρακτηρίζονται από αυξημένου βαθμού επεμβατικότητα στην ιδιωτική ζωή των καταναλωτών, λόγω του κατεξοχήν οικιακού τους χαρακτήρα και εκφράζει επιφυλάξεις με τη συμβατότητα τέτοιου είδους επεξεργασίας με τη νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα.[11]

07. Επίλογος

Συμπερασματικά προκύπτει ότι η αγορά των «έξυπνων» συσκευών εμφανίζει μεγάλα ποσοστά συγκέντρωσης σε λόγους συμμετέχοντες. Οι τεχνολογικοί κολοσσοί διαθέτοντας ανεπτυγμένα λειτουργικά συστήματα, προνομιακές τεχνολογίες και φωνητικούς βοηθούς, είναι σε θέση να υπαγορεύουν όρους και προϋποθέσεις πρόσβασης τρίτων σε αυτές κατά το δοκούν.

[9] Ibid 6.5 “The expected evolution of standardization in the near future”
[10] Ibid 7.3.5.1 “Digital advertising” & 7.3.5.2 “Consumer profiling”
[11] Ibid 7.4 “Key Findings”

Τ. 1 (2021)
E-ISSN: 2732-6004
Available online at: http://ejournals.lib.auth.gr/infolawj/

Η έρευνα είναι ακόμη σε εξέλιξη, ωστόσο ενδιαφέρον παρατηρείται από την προσωπική άποψη που εξέφρασε η επικεφαλής της Επιτροπής Ανταγωνισμού Margrethe Vestager, η οποία υποστήριξε ότι οι ισχυρές εταιρείες τεχνολογίας θα πρέπει να επιτρέψουν περισσότερο ανταγωνισμό στις πλατφόρμες τους μέσω της συμμόρφωσης σε νέους σχετικούς Κανονισμούς.

Οι τελευταίοι θα υιοθετούν μερικά κριτήρια ποσοτικά ή ποιοτικά, η εκπλήρωση των οποίων θα χαρακτηρίζει μια οντότητα ως "gate keeper" και θα συνεπάγεται τη συμμόρφωσή της με επιταγές, πχ στην περίπτωση της Apple τη δημιουργία και δεύτερου App Store για εφαρμογές τρίτων.[12]

**Ταμβάκης Νικόλαος**, Δικηγόρος, Υπ. ΔΝ

## Γ. ΠΡΟΓΡΑΜΜΑ ΔΙΑΥΓΕΙΑ: Η ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΕΠΙΒΑΛΛΕΙ ΠΡΟΣΤΙΜΟ (ΑΠΟΦΑΣΗ 21/2021 ΤΜΗΜΑ)

Στην απόφαση 21/2021, η Αρχή Προστασίας Δεδομένων επέβαλλε πρόστιμο σε ΝΠΔΔ διότι δεν απάντησε σε αίτημα διαγραφής υπαλλήλου σχετικά με ανάρτηση στο πρόγραμμα Διαύγεια που τον αφορούσε, παρά το γεγονός ότι το αίτημά του ήταν νόμιμο. Στην απόφαση συζητήθηκαν επίσης ενδιαφέροντα νομικά ζητήματα σχετικά με το είδος των ατομικών πράξεων που επιβάλλεται να δημοσιευτούν στο Πρόγραμμα Δι@υγεια, τη νομική βάση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα προκειμένου να πραγματοποιηθούν τέτοιες δημοσιεύσεις.

Σύμφωνα με τα πραγματικά περιστατικά, ο καταγγέλων ήταν υπάλληλος του ΝΠΔΔ. Είχε υποβάλλει στο ΝΠΔΔ αίτημα διαγραφής απόφασης του ΔΣ του ΝΠΔΔ που τον αφορούσε η οποία είχε αναρτηθεί στο πρόγραμμα Διαύγεια. Όπως ανέφερε, η ανάρτηση της απόφασης δεν ήταν νόμιμη καθώς δεν συνέτρεχαν οι διατάξεις σχετικά με την δημοσίευσή της, αλλά αντίθετα είχε χαρακτήρα εκδίκησης εναντίον του λόγω προηγούμενων διαφορών ανάμεσα στον εργαζόμενο και τον φορέα. Η απόφαση του Δ.Σ έθιγε τα προσωπικά του δεδομένα καθώς περιελάμβανε διάφορους μειωτικούς χαρακτηρισμούς για τον ίδιο στην εργασία του.

[12] Βλ. σχετικό δημοσίευμα εδώ.

Τ. 1 (2021)
E-ISSN: 2732-6004
Available online at: http://ejournals.lib.auth.gr/infolawj/

Στο αίτημα του υπαλλήλου, ο φορέας, ως υπεύθυνος επεξεργασίας προσωπικών δεδομένων, δεν απάντησε, παρά το γεγονός ότι είχε υποχρέωση να το εξετάσει και εντός προθεσμίας, είτε να το κάνει δεκτό και να ανακαλέσει την ανάρτηση είτε να αρνηθεί αιτιολογημένα, όπως προβλέπουν τα άρθρα 12 και 17 παρ. δ του ΓΚΠΔ. Κατά της παράλειψης του υπεύθυνου επεξεργασίας να εξετάσει το αίτημα και να αποφανθεί αιτιολογημένα, ο υπάλληλος υπέβαλλε καταγγελία στην Αρχή Προστασίας Δεδομένων. Η Αρχή Προστασίας Δεδομένων, αφού προηγουμένως εξέτασε και τους ισχυρισμούς του ΝΠΔΔ, έκρινε ότι η δημοσίευση της απόφασης του Δ.Σ, ως ατομικής διοικητικής πράξης, στο Πρόγραμμα Διαύγεια δεν ήταν νόμιμη. Συγκεκριμένα, το άρθρο 2 παρ. 4 περ. 22 του προισχύοντος νόμου 3861/2010, περιλαμβάνει την ανάρτηση των ατομικών διοικητικών πράξεων στο Πρόγραμμα Δι@υγεια, χωρίς ωστόσο αυτό να σημαίνει ότι όλες οι ατομικές διοικητικές πράξεις δημοσιεύονται εκεί. Αντίθετα, ο φορέας ως υπεύθυνος επεξεργασίας οφείλει σε κάθε μεμονωμένη περίπτωση να εξετάζει αν η ατομική διοικητική πράξη ανήκει στις κατηγορίες των πράξεων οι οποίες σύμφωνα με ειδική διάταξη νόμου δημοσιεύονται.

Το ΝΠΔΔ θα έπρεπε συνεπώς να είχε διερευνήσει αν είτε α) ο ειδικός κανόνας δικαίου που ρύθμιζε την έκδοση της εν λόγω πράξης ανέφερε ότι αυτή θα πρέπει να δημοσιευτεί είτε β) εμπίπτει σε άλλες κατηγορίες ατομικών διοικητικών πράξεων που περιλαμβάνονταν σε γενικότερους κανόνες δικαίου, όπως το άρθρο 7 Ν. 3469/2006, οι οποίες θα πρέπει να δημοσιεύονται στην Εφημερίδα της Κυβέρνησης είτε στον ημερήσιο τύπο, είτε στην ιστοσελίδα ή στο κατάστημα του φορέα. Αντίθετα το ΝΠΔΔ θεωρώντας εσφαλμένως ότι κάθε ατομική διοικητική πράξη εμπίπτει σε αυτή την κατηγορία, προχώρησε στην ανάρτηση της πράξης και δεν αιτιολόγησε το νομικό έρεισμα αυτής της απόφασης όταν ο υπάλληλος και καταγγέλων υπέβαλλε το αίτημά του για την διαγραφή της, ούτε ικανοποίησε το αίτημά του. Με τον τρόπο αυτό παραβίασε τις υποχρεώσεις του ως υπεύθυνου επεξεργασίας που απορρέουν από τον ΓΚΠΔ ως προς την υποχρέωση λογοδοσίας και προστασίας των δικαιωμάτων του υποκειμένου των δεδομένων και ειδικότερα της άσκησης του δικαιώματος διαγραφής.

Επιπλέον η χρήση των αρχικών του ονόματος του υπαλλήλου εκ μέρους του ΝΠΔΔ στην ανάρτηση του προγράμματος Δι@υγεια, δεν θεωρήθηκε επαρκές τεχνικό ή οργανωτικό μέτρο ώστε να εξασφαλιστεί **ο πλήρης και μη αναστρέψιμος αποκλεισμός ταυτοποίησής** του, καθώς από την σύνθεση και των υπόλοιπων στοιχείων που δημοσιεύτηκαν και τη διασταύρωσή τους μπορούσε να αποκαλυφθεί

Τ. 1 (2021)
E-ISSN: 2732-6004
Available online at: http://ejournals.lib.auth.gr/infolawj/

η ταυτότητά του. Κατά συνέπεια η Αρχή Προστασίας δεν έκανε δεκτό τον ισχυρισμό του ΝΠΔΔ ότι ανωνυμοποίησε τα προσωπικά δεδομένα του υπαλλήλου.

Περαιτέρω η απόφαση έχει ενδιαφέρον για την ανάλυση που παρέχει σε σχέση με την νομική βάση της επεξεργασίας των δεδομένων από δημόσιους φορείς και τη διαφορά ανάμεσα στο δημόσιο καθήκον την νομική υποχρέωση και το έννομο συμφέρον. Συγκεκριμένα, αναφορικά με τη νομική βάση για την επεξεργασία προσωπικών δεδομένων του υπαλλήλου το ΝΠΔΔ η Αρχή έκρινε ότι παρά το γεγονός ότι η παρ.1 περίπτωση γ του άρθρου 6 του ΓΚΠΔ («η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας»), έχει εφαρμογή στις περιπτώσεις που δημόσιοι φορείς επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, δεν είχε εφαρμογή στην συγκεκριμένη περίπτωση καθώς όπως αναφέρθηκε, τέτοια νομική υποχρέωση (ανάρτησης της εν λόγω πράξης) δεν υπήρχε. Ως προς την επίκληση της νομικής βάσης για την νομιμότητα της συγκεκριμένης επεξεργασίας που συνίσταται στους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας, η Αρχή παρατήρησε σχετικά ότι η εν λόγω νομιμοποιητική βάση δεν δύναται να γίνει δεκτή διότι οι πράξεις που αναρτώνται στο πρόγραμμα Δι@υγεια προβλέπονται ρητώς και δεν μπορεί να έχει ως έρεισμα την κρίση των φορέων και τα ίδια έννομα συμφέροντά τους. Στην αντίθετη περίπτωση θα υπήρχε πλήρης αντίθεση με την αρχή της νομιμότητας σύμφωνα με την οποία οι δημόσιοι φορείς μπορούν να κάνουν μόνο ότι τους επιτρέπει ρητά ο νόμος στον αντίποδα με τους ιδιώτες, οι οποίοι μπορούν να πράττουν ότι δεν τους απαγορεύει ο νόμος. Όπως συμπλήρωσε η Αρχή, σύμφωνα με τις Κατευθυντήριες Γραμμές της ΟΕ Α29 αναφορικά με το έννομο συμφέρον του υπευθύνου επεξεργασίας, στις οποίες διευκρινίζεται ότι το «συμφέρον» καταρχάς πρέπει να είναι νόμιμο, δηλαδή συμβατό, «από το ενωσιακό δίκαιο ή το δίκαιο κράτους μέλους». Για το λόγο αυτό σύμφωνα και με την αιτιολογική σκέψη 47 του ΓΚΠΔ η συγκεκριμένη νομική βάση δεν θα πρέπει να έχει εφαρμογή στις περιπτώσεις που ο υπεύθυνος της επεξεργασίας είναι δημόσιες αρχές κατά την εκπλήρωση των καθηκόντων τους.

**Κιορτσή Παναγιώτα**, Δικηγόρος, υπ. Δ.Ν.

Τ. 1 (2021)
E-ISSN: 2732-6004
Available online at: http://ejournals.lib.auth.gr/infolawj/

## Δ. ΟΙ ΥΒΡΙΔΙΚΕΣ ΑΠΕΙΛΕΣ ΚΑΙ ΟΙ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΣΕ ΥΠΟΔΟΜΕΣ

Σε ψήφισμα που εγκρίθηκε την Πέμπτη, το Ευρωπαϊκό Κοινοβούλιο ζητά τα συνδεδεμένα προϊόντα και οι συναφείς υπηρεσίες, συμπεριλαμβανομένων των αλυσίδων εφοδιασμού, να καταστούν ασφαλή εκ σχεδιασμού, και συμβάντα στον κυβερνοχώρο να θωρακίζονται γρήγορα όταν εντοπίζονται τρωτά σημεία.

Οι ευρωβουλευτές χαιρετίζουν τα σχέδια της Ευρωπαϊκής Επιτροπής να προτείνει οριζόντια νομοθεσία σχετικά με τις απαιτήσεις κυβερνοασφάλειας για συνδεδεμένα προϊόντα και συναφείς υπηρεσίες, αλλά επιθυμούν επίσης να προσπαθήσει να εναρμονίσει τις εθνικές νομοθεσίες προκειμένου να αποφευχθεί ο κατακερματισμός της ενιαίας αγοράς.

Στο κείμενο που υιοθετήθηκε το Κοινοβούλιο ζητά επίσης νομοθεσία που να θεσπίζει απαιτήσεις κυβερνοασφάλειας για εφαρμογές, λογισμικό, ενσωματωμένο λογισμικό (που ελέγχει διάφορες συσκευές και μηχανήματα τα οποία δεν είναι υπολογιστές) και λειτουργικά συστήματα (λογισμικό που εκτελεί βασικές λειτουργίες υπολογιστή) έως το 2023.

Οι ευρωβουλευτές προειδοποιούν ότι οι υβριδικές απειλές, δηλαδή μέθοδοι ή δραστηριότητες που χρησιμοποιούνται από εχθρικούς κρατικούς ή μη κρατικούς φορείς οι οποίοι στοχεύουν δημοκρατικά κράτη και θεσμούς, αυξάνονται και εξελίσσονται ολοένα και περισσότερο. Σε αυτές περιλαμβάνονται η χρήση εκστρατειών παραπληροφόρησης και οι κυβερνοεπιθέσεις σε υποδομές, οικονομικές διαδικασίες και δημοκρατικούς θεσμούς. Εκφράζουν ως εκ τούτου τις σοβαρές τους ανησυχίες για τον αντίκτυπο που μπορούν να έχουν οι εν λόγω απειλές σε εκλογικές και νομοθετικές διαδικασίες, στην επιβολή του νόμου και τη δικαιοσύνη.

Επιπρόσθετα, η κρίση COVID-19 ανέδειξε εκ νέου τα τρωτά σημεία ορισμένων κρίσιμων τομέων στον κυβερνοχώρο, ιδίως όσον αφορά την παροχή υπηρεσιών υγείας, καθώς η τηλεργασία και η κοινωνική απόσταση έχουν αυξήσει την εξάρτησή μας από τις ψηφιακές τεχνολογίες και τη συνδεσιμότητα. Οι ευρωβουλευτές τονίζουν την πρόσφατο μεγάλο αριθμό κυβερνοεπιθέσεων σε εθνικά συστήματα υγείας, όπως στην Ιρλανδία, τη Φινλανδία και τη Γαλλία, οι οποίες έχουν προξενήσει σημαντικές ζημιές στα συστήματα περίθαλψης και την φροντίδα των ασθενών.

T. 1 (2021)
E-ISSN: 2732-6004
Available online at: http://ejournals.lib.auth.gr/infolawj/

Πηγή: Επικαιρότητα, Ευρωπαϊκό Κοινοβούλιο

https://www.europarl.europa.eu/news/el/press-room/20210604IPR05531/enischusi-tis-asfaleias-stin-ee-gia-tin-antimetopisi-apeilon-ston-kuvernochoro